Claims:

1. A method for dividing a workstation into a set of separate machines such that each member of the set of separate machines is autonomous, activated separately in time (i.e. not simultaneously active with other members of the set of separate machines), and does not exchange information with other members of the set of separate machines, wherein any member of the set of separate machines can be connected to external information systems and resources without contamination (from signals from such external systems and resources) of other members of the set of separate machines, comprising the steps of:

a. connecting a separate mass-storage device (for each separate machine) to the workstation, wherein said separate mass-storage device contains the configuration and boot/start-up commands specific to its particular separate machine;

b. inserting a mass-storage device selector into the workstation, such that said selector function activates a subset of mass-storage devices connected to the workstation and deactivates mass-storage devices (connected to the workstation) not in the subset of activated mass-storage devices;

c. configuring the mass-storage device selector to initiate a workstation boot/start-up sequence as a stage of each mass-storage device selection sequence, wherein the boot/start-up sequence is a workstation reset function which prevents any information exchange between members of the set of separate machines;

d. disabling any external connectivity of the workstation during a mass-storage

device selection sequence, such that no hostile external information signals impact the workstation during said selection sequence;

e. restoring deactivated mass-storage devices to an initial non-contaminated state;

2. The method of claim 1, wherein the step of connecting includes external (to the workstation) and internal (to the workstation) mass-storage devices, whereby such mass-storage devices range from standard hard-disk drive (HDD) units to removable media devices such as tape drives, ZIP drives, CD-R drives, CD-R/W drives, writeable DVD drives, and like devices;

3. The method of claim 1, wherein the step of inserting and the step of configuring includes the implementation of an optional access control function (e.g. lock & key) for the mass-storage device selector, thus enabling the capability to restrict certain users (of a workstation) to specific members of the set of separate machines, of a multiple user workstation, thereby forcing a degree of privacy protection for the multiple users of said workstation;

4. The method of claim 2, wherein a mass-storage device is treated as a logical mass-storage unit and can include a multiplicity of mass-storage devices connected in such manner as to operate as a single mass-storage unit (e.g. a master-slave configuration), defining a single member of the set of separate machines of a

workstation;

5. A system for dividing a workstation into a set of separate machines such that each member of the set of separate machines is autonomous, activated separately in time (i.e. not simultaneously active with other members of the set of separate machines), and does not exchange information with other members of the set of separate machines, wherein any member of the set of separate machines can be connected to external information systems and resources (such as the Internet) without contamination (from signals from such external systems and resources) of other members of the set of separate machines, comprising:

a. a means for connecting a separate mass-storage unit (for each separate machine) to the workstation, wherein said separate mass-storage unit contains the configuration and boot/start-up commands specific to its particular separate machine;

b. a means for selecting separate mass-storage units connected to the workstation, such that said means for selecting activates a subset of mass-storage units connected to the workstation and deactivates mass-storage units (connected to the workstation) not in the subset of activated mass-storage units;

c. a means for initiating a workstation boot/start-up sequence as a stage of each mass-storage unit selection sequence, such that the boot/start-up sequence is a workstation reset function which prevents any information exchange between members of the set of separate machines;

d. a means to disable external connectivity of the workstation during a mass-

storage unit selection sequence, such that no hostile external information signals impact the workstation during said selection sequence;

e. a means for restoring deactivated mass-storage units to an initial non-contaminated state;

6. The system of claim 5, wherein a mass-storage unit defining a member of the set of separate machines of a workstation, is comprised of a multiplicity of mass-storage devices connected in such manner as to operate as a single mass-storage unit, whereby the multiplicity is comprised of mass-storage devices that range from standard hard-disk drive (HDD) units to removable media devices such as tape drives, ZIP drives, CD-R drives, CD-R/W drives, writeable DVD drives, and like devices;

7. The system of claim 5, wherein the means for selecting implements an exclusive-OR (i.e. XOR) type process, such that *at most* one member of the set of separate machines (of the workstation) is active at any time;

8. The system of claim 5, wherein the means for initiating is an automatic step of the mass-storage unit selection process;

9. The system of claim 5, wherein the means for restoring is a user-optional, application-specific, function which generically involves a disk-copy type process, such that the deactivated mass-storage unit receives an image/copy of the contents of a

base mass-storage unit connected to the workstation;

10. The system of claim 9, wherein a base mass-storage unit is defined at operational initiation of the workstation and is a member of the set of separate machines (of the workstation) which is available only for the mass-storage unit restoration process, and is not available for selection as the component of an operational separate machine;

11. The system of claim 10, wherein a multiplicity of base mass-storage units is defined;

12. The system of claim 5, wherein the means for connecting includes the means for connecting a multiplicity of mass-storage units, each of which is structured as a full computer system (such as an embedded computer type device, a single board computer type device, or like devices), in such manner that each of the separate machines operates as an autonomous embedded unit to the host workstation, wherein each embedded unit has the functionality of a complete computer system of its type (e.g. single board computers, PC/104 type embedded computers, PC/104-+ type embedded computers), in addition to its mass-storage unit function;

13. The system of claim 12, wherein each member of the set of computer-system-structured mass-storage units has the capability to be reset by the selection

process of claim 5, at the time of its selection, whereby the initiation (including automatic initiation) of an actual reset function is an application specific determination by users of the workstation;

14. The system of claim 12, wherein each computer-system-structured mass-storage unit is configured in such manner that its separate machine interfaces with a different external resource, wherein each of said external resources is classified (e.g. Top Secret, Confidential, Proprietary, project-λ, etc.), thus implementing a CMWS (Compartmented Mode WorkStation) capability; for the workstation;

15. The system of claim 14, wherein each computer-system-structured mass-storage unit has the capacity to filter outgoing information signals from its separate machine, thereby preventing unauthorized release of information;

16. The system of claim 5, wherein each separate machine is physically separated from all other separate machines connected to the workstation, thus further reducing the probability of information exchange between the separate machines connected to the workstation, wherein such physical separation is a property of the architecture of the invention;

17. The system of claim 12, wherein members of the set of computer-system-structured mass-storage units are independently configured to perform functions such

as floating-point computation, pattern matching, virtual streaming, and like advanced functions either computationally-based or non-computationally-based (e.g. dynamic pattern matching/classification functions), such that the selection/activation of said units enables computing clusters, thus providing adaptive advanced functionality to the workstation;

18. The system of claim 16, wherein each physically-separated separate machine defined by a computer-system-structured mass-storage unit, hosts its own software operating-system (such as Windows, Linux, or like software operating-systems), thus creating and maintaining a separate isolated domain for said operating-system, whereby a particular software operating-system hosted by a member of the set of separate machines of a workstation may be identical to that operating-system hosted by another member of the set of separate machines of said workstation, without exchange of information signals between such members of the set of separate machines of the workstation;

19. The system of claim 18, wherein the confinement of a specific operating-system (such as Windows, Linux, etc.) to a particular separate machine of the host workstation, also confines any peculiarities, errors, incompatibilities, contamination, and such deficiencies (of an operating-system), to that particular separate machine, thereby adding an element of Fault-Tolerance to the host workstation;

20. The system of claim 19, wherein the use of the separate machines provides the users of the host workstation an operational bridge between incompatible external (to the workstation) resources, wherein this operational bridge provides a "virtual interoperability" capability between incompatible external resources, whereby such external resources can include various incompatible "instant messaging" type systems, providing relief to the problem of incompatibility of such external resources;

21. The system of claim 20, wherein a subset of the set of separate machines of a workstation are configured to store and process internal (e.g. classified, proprietary, etc.) information, wherein such configuration restricts connectivity (of members of this subset of separate machines) to corporate local-area-network (LAN) type resources or other like internal/private resources, thereby defining a subset of protected separate machines;

22. The system of claim 21, wherein a subset of the set of separate machines of a workstation are configured to store and process internal (e.g. classified, proprietary, etc.) information, wherein such configuration restricts connectivity (of members of this subset of separate machines) to operate in a stand-alone mode (i.e. zero external, to the workstation, connectivity), thereby defining a subset of stand-alone, protected separate machines, whereby a stand-alone operational mode is generically the most secure from external contamination and hacker type attack.